REMARKS

By the foregoing amendments, Applicants have revised claims 1, 22, 41, 61, 71, 76, and 84 in such a manner as to define the invention more accurately, they have canceled claim 65 and revised claim 68 to eliminate resultant redundancy, and they have changed the dependencies of claims 66 and 67, which depended on now-canceled claim 65. Claims 1-64 and 66-84 remain after the amendment.

Applicants additionally have so revised claim 84 as to eliminate the basis for the Office action's § 112 rejection. Specifically, that claim is now directed more clearly to a storage medium containing instructions for performing the recited operations. Applicants therefore request that the Examiner withdraw his §112 rejection.

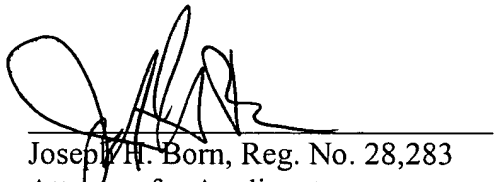
Applicants' independent claims define an approach to message-tampering prevention that does not require expensive cryptographically strong integrity functions. The Examiner has rejected all of those claims as defining subject matter anticipated by the system described in U.S. Patent No. 5,850,449 to McManis. Applicants respectfully request that the Examiner reconsider this rejection, because the McManis arrangement does not provide the recited features, so it can prevent tampering only by using cryptographically strong—and therefore expensive-to-compute—functions to produce the digest that it employs.

Specifically, as lines 55-58 et seq. of McManis's column 5 indicate, the message digest that McManis generates by, among other things, applying a hash function to the message being sent can be decrypted by using a public key. McManis therefore does not prevent an interloper from inspecting the digest; the interloper need only use the sender's public key in order to decrypt it. So, if the interloper can arrive at a message that hashes to the digest's value, he can change the message without detection. The hash function therefore has to be cryptographically strong if tampering is to be prevented.

In contrast, Applicants keep the integrity-function output secret. Applicants can therefore use cryptographically weak—and therefore inexpensive-to-compute—integrity-check functions, because the interloper is unable to inspect the hash function's output.

All independent claims now define this concept. As claim 1 now recites, for example, "the integrity block processor . . . so encrypts the one or more integrity checks . . . as to permit their decryption only with a non-public key. . . ." The prior art on which the Examiner relies neither discloses nor suggests this concept, so those claims and all the claims that depend on them define subject matter patentable over the prior art of record. Applicants therefore reconsider and allow all remaining claims.

Respectfully submitted,



Date: July 23, 2004
Customer No: 25181
Patent Group
Foley Hoag, LLP
155 Seaport Blvd.
Boston, MA 02210-2600

Joseph H. Born, Reg. No. 28,283
Attorney for Applicants
Tel. No. (617) 832-1134
Fax. No. (617) 832-7000